APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,465	09/14/2005	Junbiao Zhang	PU030083	8383

24498   7590   04/13/2010

Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER
ZIA, SYED

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/13/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<table>
<tr><td rowspan="3">Office Action Summary</td><td>Application No.
10/549,465</td><td>Applicant(s)
ZHANG ET AL.</td></tr>
<tr><td>Examiner
SYED ZIA</td><td>Art Unit
2431</td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 October 2009*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This office action is in response to amendments and remarks filed on October 2, 2009.

Claims 1-27 are pending.

Response to Arguments

Applicant's arguments filed on October 2, 2009 have been fully considered but they are

not persuasive because of the following reasons:

Regarding Claims 1 applicants argued that the cited prior art does not teach "*determining*

whether the user terminal uses a predetermined authentication protocol in response to the

response to the identity request message; and selecting an authentication mechanism

compatible with the user terminal upon determining the user terminal is not compatible with the

predetermined authentication protocol, for allowing user terminal access to the

communications network". Applicant also argued that cited prior art does not teach

"*determining whether the mobile terminal is IEEE 802 is compliant in response to the response*

to the identity request message; and selecting an authentication mechanism, compatible with

the mobile terminal, in response to a determination that the mobile terminal is not IEEE 802. 1

is compliant, for allowing user mobile terminal access to the wireless local area network"

This is not found persuasive. The system of cited prior art teaches a system and method

and apparatus for accessing networks by a mobile device. The carrier network uses the user

information to authenticate the user and to generate session data while the user is accessing the

carrier network. In addition, the access point database includes information about the signal

types or protocol used by the carrier network. For example, whether the carrier network uses

IEEE 802.11b as opposed to 802.11g as its protocol. The carrier network transmits the session

data to the access server. The access client further includes access point detection and evaluation

features for use by a user in selecting access points available at a single location. In access client

the mobile computing device is operably coupled to a carrier network via a communications link

adapted for communication using a wireless protocol such as IEEE 802.11b. The

communications link may be established via a medium such as radio wave or infrared

transmissions. The method cited prior art also involves generating a user selectable list of

multiple carrier network identifiers e.g. service set identifier, by an access client using carrier

network information, where the identifiers associated with a common carrier network system are

aggregated to generate a carrier network system identifier that is included in the list. The

information is obtained from an access point database by the client using the identifiers, where

the information includes information of whether the access client is authorized to access one of a

set of carrier networks (col. 5 line 54 to col.6 line 8, col.9 line 10 to line 35, col. 11 line 1 to

col.12 line 7, and col.16 line 35 to col.18 line 40).

Thus the system of cited prior art provides a system and method for controlling access by

a mobile terminal to a WLAN by accommodating for each mobile terminal its particular

capabilities and selecting accordingly,

Therefore, the examiner asserts that cited prior art does teach or suggest the subject

matter recited in independent and dependent claims. Accordingly, rejections for claims 1-27 are

respectfully maintained.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1.   Claims 10-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 10-13 are not statutory because they are directed towards an access point to determine whether the terminal device utilizes a protocol, which could be implemented via software alone. Claims to software per se are not statutory.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim1, 6, 11-16, 18, 21-23, and 25-27 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. These claims are based on conditional statements which make them indefinite because it is not clear what will happen when this condition is not satisfied. Some examples are: Clam 1: *selecting an authentication mechanism compatible with the user terminal upon determining the user terminal is not compatible with the predetermined authentication protocol.* Claim 6: *if the mobile terminal is not IEEE 802.1x compliant,*

redirecting an authentication request to an HTTP server for utilizing a browser based

authentication. Clam 13: " *if the access point detects that the terminal device is an IEEE 802.1x*

client". Claim 14: *and if the terminal device utilizes an IEEE 802.1x protocol.*

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Jonker et al.

(U.S. Patent 7,483,984).

1.   Regarding Claim 1 Jonker teach and describe a method for controlling access by a user

terminal to a communications network comprising the steps of: receiving from the user terminal

a request to access the communications network; transmitting to the user terminal an identity

request message; receiving from the user terminal, a response to the identity request message;

determining whether the user terminal uses the predetermined authentication protocol in

response to the response to the identity request message; selecting an authentication mechanism

compatible with the user terminal upon determining the user terminal is not compatible with the

predetermined authentication protocol, for allowing user terminal access to the communications

(col. 5 line 54 to col.6 line 8, col.9 line 10 to line 35, and col. 11 line 1 to col.12 line 7).

2.   Regarding Claim 4 Jonker teach and describe method for controlling mobile terminal

access to a wireless local area network, comprising the steps of: receiving from the mobile

terminal a request to access the wireless local area network; transmitting to the mobile terminal

an identity request message; receiving from the mobile terminal, a response to the identity

request message; determining whether the mobile terminal is IEEE 802.1x compliant in response

to the response to the identity request message; and selecting an authentication mechanism,

compatible with the mobile terminal in response to a determination that the mobile terminal is

not IEE 802.1x compliant, for allowing user mobile terminal access to the wireless local area

network (col. 5 line 54 to col.6 line 8, col.9 line 10 to line 35, and col. 11 line 1 to col.12 line 7).

3.   Regarding Claim 10 Jonker teach and describe an access point in communication with a

terminal device in a wireless local area network, comprising: a means to determine whether the

terminal device utilizes an IEEE 802.1x protocol and, if the terminal does not utilize said

protocol, then the access point employing an authentication means compatible with the terminal

device otherwise the access point employing an IEEE 802.1x protocol (col. 5 line 54 to col.6 line

8, col.9 line 10 to line 35, and col. 11 line 1 to col.12 line 7).

4.   Regarding Claim 14 Jonker teach and describe a method for controlling access by a

terminal device in a wireless local area network by determining whether the terminal device

utilizes an IEEE 802.1x protocol comprising the steps of: an access point communicating to the

mobile terminal a request to identify, and if the terminal device utilizes an IEEE 802.1x protocol,

acknowledging the request to identify, otherwise the access point determining that the terminal is

not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the

mobile terminal (col. 5 line 54 to col.6 line 8, col.9 line 10 to line 35, and col. 11 line 1 to col.12

line 7).

5.   Regarding Claim 21 Jonker teach and describe a method for controlling access of a

terminal device in a wireless local area network by determining whether the terminal device

utilizes an IEEE 802.1x protocol comprising the steps of: communicating through the an access

point to the mobile terminal a request to identify, and if the terminal device utilizes an IEEE

802.1x protocol, acknowledging the request to identify, otherwise determining by the access

point that the terminal is not IEEE 802.1x compliant and selecting an authentication mechanism

compatible with the terminal (col. 5 line 54 to col.6 line 8, col.9 line 10 to line 35, and col. 11

line 1 to col.12 line 7).

6.   Claims 2-3, 5-9, 11-13, 15-20, , and 22-27are rejected applied as above rejecting Claims

1, 4, 10, 14, and 21. Furthermore, Jonker teach and describe a, wherein:

As per Claim 2, the user terminal comprises a mobile terminal and the communications

network comprises a wireless local area network wireless local area network that complies with

the IEEE 802.11 standards (col. 5 line 54 to col.6 line 8).

As per Claim 3, the selecting step includes selecting an appropriate authentication server coupled to the wireless local area network in response to the determination (.col.4 line 1 to col. 5 line 17).

As per Claim 5, further comprising the steps of, if the mobile terminal is IEEE 802.1x compliant, transmitting an authentication request to an authentication server and receiving an authentication response utilizing the IEEE 802.1x protocol, and controlling mobile terminal access to the wireless local area network in response to the authentication response (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8).

As per Claim 6, further comprising the steps of, if the mobile terminal is not IEEE 802.1x compliant, redirecting an authentication request to an HTTP server for utilizing a browser based authentication (col.4 line 1 to col.5line 17, and col.16 line 35 to col.18 line 40).

As per Claim 7, further comprising the step of configuring a packet filtering module to redirect the authentication request to the HTTP server (col.16 line 35 to col.18 line 40)..

As per Claim 8, further comprising the step of maintaining state information in the wireless local area network for use by the packet filtering module and the HTTP server (col.16 line 35 to col.18 line 40).

As per Claim 9, the state information includes one of a first state indicative of ongoing authentication process, a second state indicative of authentication failure, a third state indicative of authentication success, and a fourth state indicative of a non IEEE 802.1x mobile terminal (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8)

As per Claim 11, wherein the means to determine includes communicating to the terminal device a Request-Identity extensible authentication protocol packet and if the mobile terminal

utilizes the IEEE 802.1x protocol the access receives a Response-Identity extensible

authentication protocol packet (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8)

As per Claim 12, further comprises the means to configure an internet protocol packet

filtering to redirect the device HTTP request to a local server if the terminal device does not

utilize said protocol (col.16 line 35 to col.18 line 40).

As per Claim 13, The access point in claim 10, further comprises means to communicate

IEEE 802.1x protocol exchanges and means to establish internet protocol packet filtering

through an internet protocol filter module and state information for the HTTP server to control

the terminal device access during and after IEEE 802.1x based authentication process if the

access point detects that the terminal device is an IEEE 802.1x client (col.4 line 1 to col. 5 line

17, and col. 5 line 54 to col.6 line 8, and col.16 line 35 to col.18 line 40).

As per Claim 15, wherein the access point determines that the terminal is not IEEE

802.1x compliant when it does not receive an extensible authentication protocol identity

response packet after a timeout value (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line

8).

As per Claim 165, further comprising the step of access point detecting that if the

terminal device is not IEEE 802.1x compliant, then configuring an internet protocol packet filter

and redirecting a user HTTP request to a local server (col.4 line 1 to col.5line 17, and col.16 line

35 to col.18 line 40)..

As per Claim 17, further comprising the step of the local server communicating to the

terminal device information specifically related to a browser based authentication (col.16 line 35

to col.18 line 40).

As per Claim 18, further comprising the step of the access point transitioning to a state if the terminal device utilizes the IEEE 802.1x protocol that indicates that the terminal device is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8).

As per Claim 19, further comprising the step of the access point transitioning to a state corresponding to browser based authentication if the authentication process fails (col.16 line 35 to col.18 line 40).

As per Claim 20, further comprising the step of the access point transitioning to a state corresponding to browser based authentication if the terminal device is not IEEE 802.1x compliant (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8).

As per Claim 22, further comprising the step of deter-mining in the access point that terminal is not IEEE 802.1x compliant if it does not receive an extensible authentication protocol identity response packet after a preset time (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8).

As per Claim 23, further comprising the step of detecting in the access point that if the terminal device is not IEEE 802.1x compliant, then configuring an internet protocol packet filter and redirecting a user HTTP request to a local server (col.4 line 1 to col.5line 17, and col.16 line 35 to col.18 line 40).

As per Claim 24, further comprising the step of communicating from the local server to the terminal device, information specifically related to a browser based authentication (col.16 line 35 to col.18 line 40).

As per Claim 25, further comprising the step of transitioning to a state in the access point if the terminal device utilizes the IEEE 802.1x protocol that indicates that the terminal device is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8).

As per Claim 26, further comprising the step of transitioning to a state in the access point corresponding to browser based authentication if the authentication process fails (col.16 line 35 to col.18 line 40).

As per Claim 27, further comprising the step of transitioning to a state in the access point corresponding to browser based authentication if the terminal device is not IEEE 802.1x compliant (col.4 line 1 to col. 5 line 17, and col. 5 line 54 to col.6 line 8)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
April 2, 2010
/Syed   Zia/
Primary Examiner, Art Unit 2431